



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

FOR INTERNAL USE

Holder of information: Data Protection Inspectorate

Notation made: [REDACTED].2025

The access restriction shall be valid until: [REDACTED] 2030
for p 2 until entry into force of the DecisionLegal ground: Section 35(1)(2), Section 35(1)(9),
Section 35(1)(18²) of the PIA

All SA's

[REDACTED].2025 No. [REDACTED]

ARTICLE 60 FINAL ADOPTED DECISION**Termination of supervisory proceedings in the matter of personal data protection**

The Estonian Data Protection Inspectorate (the Estonian DPI) is conducting a supervisory procedure¹ in connection with a phishing attack targeted at [REDACTED] (the controller), which resulted in a personal data breach.

Circumstances of the data breach

[REDACTED] (the controller) submitted a preliminary notification to the Estonian DPI on [REDACTED] [REDACTED].2025 and a final breach notification on [REDACTED] 2025, indicating a potential data leak in the [REDACTED] system of [REDACTED] [REDACTED]. On [REDACTED] 2025, [REDACTED] informed the controller that a data leak may have occurred on [REDACTED] 2024, during which a report containing two years' worth of room bookings may have been exposed. The breach affected 2258 customers, and the leaked data may have included first and last names, email addresses, phone numbers, addresses, and countries of origin.

The controller changed all passwords, informed employees of possible issues and examined the circumstances of the possible breach in cooperation with the processor [REDACTED]. In addition, the controller contacted CERT EE and the police.

As the breach notification did not contain exhaustive information about the incident, the Estonian DPI initiated a supervisory procedure and submitted an inquiry to the controller.

Since the breach affected residents of other European Union (EU) and European Economic Area (EEA) countries, the Estonian DPI notified the relevant EU and EEA data protection authorities and initiated a procedure under Article 56(1) of the General Data Protection Regulation (GDPR) to determine the lead supervisory authority. The Estonian DPI is the lead supervisory authority, as [REDACTED] is an Estonian company with its management board located in Estonia.

Clarifications by the controller

[REDACTED] explained that it is the controller and [REDACTED] is the processor. [REDACTED] is used to manage [REDACTED] customer bookings. [REDACTED] stores the customer's first and last name, contact details (including address, e-mail, telephone), citizenship, gender, date of birth and, in the case of a non-EU, a document and its number.

¹ The Supervision Authority commenced proceedings on the basis of Section 56(1) and (3)(8) of the Personal Data Protection Act. Legal basis for requesting clarifications: Sections 57-58 of the Personal Data Protection Act, Section 30(1) and (3) of the Law Enforcement Act, and Article 58(1)(a), (e) and (f) of the General Data Protection Regulation.

² The website of the [REDACTED] service provider is [REDACTED]

On [REDACTED] 2025, [REDACTED] sent a letter to the controller stating that they had observed an increase in phishing scams and the emergence of fake [REDACTED] login pages. According to [REDACTED]' analysis, an employee of [REDACTED] had entered their login credentials on such a fake page. The letter sent by [REDACTED] also included a report indicating that, using the hotel employee's account, a booking report covering the period from [REDACTED] 2024 to [REDACTED] 2026 had been generated on [REDACTED] 2024. The hotel employee confirmed that they had not generated the report in question.

The report that may have been leaked contained data of inconsistent quality. For some customers, the report included first and last names, email addresses, and other details, while for others, only names were listed without any contact information.

Before a possible breach occurred, two-factor authentication was set mandatory for all users to protect the [REDACTED] environment's login. Antivirus and anti-malware software is installed on users' computers.

The controller asked [REDACTED] how unauthorised access to the system is possible when two-factor authentication was in place and received a reply from the processor that, as phishing actors are becoming increasingly professional, and occasionally they manage [REDACTED]

[REDACTED] holds an ISO 27001 certification, based on which [REDACTED] considered [REDACTED] to be a trustworthy and secure partner. [REDACTED] has assisted in identifying the potential breach and provided extracts. [REDACTED] has developed an online training course on Security & Phishing Attempts Protection, including the topic of fake login pages and asked all users to complete it. [REDACTED] has implemented the [REDACTED] and Trusted Device security features provided by [REDACTED] for logging in to [REDACTED], which are mandatory for all [REDACTED] users.

To prevent future possible data leaks, the controller plans to organize cybersecurity training to raise user awareness. The controller is working with a partner who conducts phishing email tests for companies (sending simulated phishing emails to users and collecting statistics).

[REDACTED] did not consider it necessary to notify the individuals affected by the breach, as they were not certain that an actual data leak had occurred. The possible data leak took place in [REDACTED] 2024 and [REDACTED] informed [REDACTED] about it in [REDACTED] 2025. As of [REDACTED] 2025, no individual has contacted the controller regarding a possible data leak and [REDACTED] therefore assumed that no actual data leak has occurred. Additionally, most of the potentially leaked bookings have been in the past. Furthermore, the controller does not possess complete data of a large number of individuals and therefore it has not been possible to notify them of a potential leak.

The position of the Estonian Data Protection Inspectorate

1. Pursuant to Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation or GDPR), personal data means any information relating to an identified or identifiable natural person (data subject). In the [REDACTED] system, [REDACTED] has customers' first and last name, contact details (including address, e-mail, telephone), citizenship, gender, date of birth, and in the case of non-EU customers, also a document and its number.
2. Pursuant to Article 4(12) of the GDPR, a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, stored or otherwise processed personal data transmitted. As a result of the phishing attack, unauthorized access to personal data was obtained, as it has been identified that a report on bookings was generated from the [REDACTED] system on behalf of a user who has not done so themselves. It is therefore a personal data breach.

3. In accordance with the principles governing the processing of personal data, namely Article 5(1)(f) of the GDPR, personal data must be processed in such a way as to ensure their appropriate security and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
4. The same obligation is further regulated in Articles 24 and 32 of the GDPR. Under Article 24(1) of the GDPR, the controller must implement appropriate technical and organisational measures to ensure and be able to demonstrate that personal data are processed in accordance with the GDPR, taking into account the nature, scope, context and purposes of the processing of personal data, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Pursuant to Article 32(1) GDPR, the controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including ensuring the continued confidentiality, integrity, availability and resilience of the systems and services processing personal data. Pursuant to Article 32(2) GDPR, the assessment of the necessary level of security shall in particular take into account the risks arising from the processing of personal data, in particular accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
5. In order to ensure security and prevent processing in breach of GDPR, the controller should assess the risks associated with the processing and implement measures to mitigate those risks. Taking into account the latest scientific and technological developments and the costs of implementing the measures, those measures should ensure an appropriate level of security, including confidentiality, appropriate to the risks and the nature of the personal data to be protected. When assessing the data security risk, consideration should be given to the risks arising from the processing of personal data, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed, which may, in particular, result in physical, material or non-material damage.³
6. No one is protected from phishing attacks, but in order to avoid it, the controller must ensure the security of the information systems and the systems must be regularly monitored to identify any risks that may have arisen. The Estonian DPI takes into account that █████ holds an international ISO 27001 certificate for information security, which gave the controller the basis to consider the processor reliable and secure. The processor monitored its systems and informed the controller about phishing. Prior to the breach, █████ had set two-factor authentication as mandatory for all users in order to protect the login to █████ environment, but the attacker managed to █████ by using fake █████' login page, which deceived the controller's employee.
7. Pursuant to Article 31 GDPR, the controller shall cooperate with the supervisory authority on request in the performance of its tasks. In accordance with Article 33(1) of the GDPR, the controller submitted a preliminary notification to the Estonian DPI within 72 hours, followed by a final notification of a data breach. The Estonian DPI submitted enquiries to █████ in the course of the proceedings, to which the controller replied and provided explanations on the circumstances of the breach.
8. Pursuant to Article 34(1) of the GDPR, the controller notifies data subjects of a breach where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. █████ did not notify the data subjects of the breach, as the data leak occurred in █████ 2024 and the controller became aware of it in █████ 2025. Most of the leaked bookings were in the past. In addition, the controller does not have the full data of

³ Recital 83 of the GDPR.

a large number of individuals and therefore it has not been possible to notify them of a potential leak. No person has contacted the controller about a possible data breach. The Estonian DPI takes into account the explanations provided by the controller and considers that the breach is unlikely to pose a high risk to the rights and freedoms of natural persons, as most of the bookings were in the past and the data reported were of inconsistent quality (e.g. name without contact details). In addition, there was no special category of personal data in the report.

9. Following the breach, the controller implemented additional security measures for [REDACTED] login, planned cybersecurity awareness training for staff, and partnered with a service provider to conduct phishing email tests.
10. The Estonian DPI is of the opinion that although a personal data breach occurred, the controller had implemented modern security measures (e.g. two-factor authentication) before the breach occurred and assessed the reliability and security of the processor, although the implemented measures did not withstand the attack. In addition to the above, the Estonian DPI considers that the controller cooperated with the Estonian DPI in the investigation of the breach, identified the cause, and has taken additional measures to prevent similar attacks.

On the basis of the above, the Estonian DPI terminates the supervisory procedure.

This notice of termination of the supervision proceedings can be challenged within 30 days by submitting an appeal to the administrative court under the Code of Administrative Court Procedure⁴.

Respectfully,

[REDACTED]

lawyer

authorized by the Director-General

⁴ <https://www.riigiteataja.ee/en/eli/ee/512122019007/consolide/current>